

# **EXHIBIT A**

# FAQ

- General

- How does Namecoin work?
- Do I need to back up my wallet?
- How much does it cost to register a domain (a.k.a. a name)?
- How do I obtain namecoins? Can I mine them?
- Who gets the registration fee?
- Who gets the transaction fee?
- How long are names good for?
- How do I browse a .bit domain?
- How do I register and host a .bit domain?
- Do I have to pay renewal fees?
- What applications is Namecoin well-suited to?
- Do I need to download the entire Namecoin blockchain to use Namecoin?
- What is the smallest currency unit of Namecoin called?
- What do Namecoin addresses look like?

- Design

- What is a namespace?
- Why is there a separate pre-registration step?
- How are names represented?
- What if I spend that special coin by mistake?
- Why does registering a name incur a fee?
- Why don't name registration fees go to miners?
- Why do names have to be renewed regularly?
- Does Namecoin support "layer 2" technologies?
- Why focus on getting browsers and OS's to support Namecoin instead of getting ISP's or public DNS resolvers (e.g. Google DNS) to do so?
- Why focus on browser add-ons and OS packages instead of native browser and OS support?
- Why focus on getting existing browsers and OS's to support Namecoin instead of forking those browsers and OS's?
- Is Namecoin's support of atomic name trades a feature primarily aimed at squatters?
- Does Namecoin have any browser add-ons?

- Why doesn't Namecoin use a WebExtension to resolve `.bit` domains to IP addresses?
- Why doesn't Namecoin use "proof of stake"?
- Comparison of Namecoin to other projects
  - What is the relationship of Namecoin to Bitcoin?
  - What is the difference between Namecoin and Bitcoin?
  - What are the similarities between Namecoin and Bitcoin?
  - Does Namecoin mandate usage of Bitcoin as a parent chain?
  - Does Namecoin influence Bitcoin's hashrate?
  - How does Namecoin compare to Tor Onion Services?
  - How does Namecoin compare to Let's Encrypt?
  - How does Namecoin compare to Blockstack?
  - How does Namecoin compare to Monero?
  - What is Namecoin's relationship to OpenNIC?
- Weaknesses
  - How easy is it for names to be stolen? What can be done if it happens?
  - What is the threat posed by 51% attacks?
  - Is squatting a problem? What can be done about it?
  - Is Namecoin anonymous?
  - I heard that an academic study found that Namecoin is only used by 28 websites; is that really true?
  - How does Namecoin affect global heating?

## General

### How does Namecoin work?

The Namecoin software is used to register names and store associated values in the blockchain, a shared database distributed by a P2P network in a secure way. The software can then be used to query the database and retrieve data.

### Do I need to back up my wallet?

If you're using Namecoin to register or otherwise own names, or to transfer namecoins, then you do need to periodically back up your wallet. Like Bitcoin, your wallet's keys are located in your `wallet.dat` file. You should encrypt this file by going to **Settings** > **Encrypt Wallet** and making a backup thereafter. Close the

Namecoin client and make a backup of your `wallet.dat` file in your Namecoin profile folder. (On GNU/Linux, this is usually `~/.namecoin/`; on Windows, it is usually `C:\Users\<Your Username>\AppData\Roaming\Namecoin\`). It is currently recommended to back up more often than every 100 transactions (including both currency and name transactions).

If you are only using Namecoin to look up names (e.g. browsing `.bit` domains), then you do not need to encrypt or back up your wallet.

## How much does it cost to register a domain (a.k.a. a name)?

The cost includes a registration fee and a transaction fee. The registration fee is 0.01 NMC, and the transaction fee is determined dynamically by miners (just like in Bitcoin). The registration fee might be made dynamic in the future, to improve economic incentives.

## How do I obtain namecoins? Can I mine them?

You can mine them alongside bitcoins or trade them, see [How to get Namecoins](#).

## Who gets the registration fee?

The registration fees are destroyed by the transaction. Nobody gets them.

## Who gets the transaction fee?

The miners do, just like in Bitcoin. Paying higher fees improves the chance that the transaction will be processed quickly. Like Bitcoin, the client will suggest a fee that is likely to be processed quickly.

## How long are names good for?

Registered names semi-expire if they are not renewed or updated for 31,968 blocks (approximately 222 days). If your name is semi-expired, it will stop resolving for your users until you renew or update it, but you are still the sole owner of the name. Semi-expired names that are not renewed or updated for an additional 4,032 blocks (approximately 28 days) will expire. Expired names can be re-registered by anyone. There are no registration fees for renewals or updates, but a transaction fee does apply.

## How do I browse a .bit domain?

See [Browsing .bit Websites](#).

You can also use [ncdns](#) (experimental). If you have the [ZeroNet](#) software installed, you can visit ZeroNet-enabled .bit domains.

## How do I register and host a .bit domain?

See [Documentation for Name Owners](#).

## Do I have to pay renewal fees?

Other than the standard transaction fee, not at the moment. This might change in the future, to improve economic incentives.

## What applications is Namecoin well-suited to?

Consider that Namecoin values are limited to 520 bytes, and that the block size limit is somewhere between 500 kB and 1 MB. (It's lower than Bitcoin's.) Given that blocks occur every 10 minutes on average (usually fluctuating between 1 and 60 minutes), and that names have to be updated or renewed at least every 35,999 blocks, try to figure out whether your application would comfortably fit into blocks if your application became widespread. Domain names and identities are applications that are near the upper limit of the scale that Namecoin can handle. For example, misusing the Namecoin blockchain as a decentralized file storage is not feasible. There are several other decentralized systems that serve this purpose way more efficiently. In many cases, if you want to store data that is larger than 520 bytes, or that is updated very often, you may prefer to only store a content hash or a public key in the blockchain, along with information on where to get the full data. The full data can then be authenticated using Namecoin as a trust anchor without storing the entire data in Namecoin. See our [Layer 2](#) documentation for examples of such usage.

If you're developing an application, consider doing your development on the Namecoin Testnet. This prevents your testing from bloating the production blockchain, and also allows you to test without spending real money on names. If more than one implementation might have the same use case, consider writing a spec so that incompatible implementations of similar ideas don't become a problem.

## Do I need to download the entire Namecoin blockchain to use Namecoin?

No, but you will get better security if you choose to do so. A *full node* such as Namecoin Core gives you maximum security by downloading the entire blockchain and validating that all transactions comply with the Namecoin consensus rules. However, if you don't wish to download the entire blockchain, you can instead use a *lightweight SPV node* such as Electrum-NMC, which only downloads block headers (along with transactions that are relevant to you), which are much smaller than the entire blockchain. Namecoin also makes possible some security models that don't directly correspond to Bitcoin. For example, the ConsensusJ-Namecoin node downloads block headers like Electrum-NMC, but also downloads the entire blocks from the past year only (i.e. all blocks that contain unexpired name transactions), which provides a security level somewhere between Electrum-NMC and Namecoin Core.

## What is the smallest currency unit of Namecoin called?

The smallest currency unit of Namecoin is called the *swartz* (similar to the *satoshi* in Bitcoin). It is named after Aaron Swartz, the activist who was murdered by the U.S. government, and who [proposed Nakanames](#) (which, along with BitDNS, described the concept that was later implemented as Namecoin).

## What do Namecoin addresses look like?

Namecoin addresses follow the same format as Bitcoin addresses, but with different prefixes (to avoid ambiguity about whether an address is for Bitcoin or Namecoin):

- New-style Bech32 addresses begin with **nc1**.
- Old-style P2SH addresses begin with **6**.
- Even-older-style P2PKH addresses begin with **N** or **M**.

## Design

### What is a namespace?

Namespaces are name prefixes used by applications to distinguish between different type of names in Namecoin. For example, **d/example** is the domain name **example.bit**, and **id/example** is an identity. Namespaces help prevent

multiple applications from accidentally conflicting. Namecoin itself isn't aware of namespaces, and namespaces don't have any effect on validation rules; they are only used by higher-level applications that use Namecoin.

## Why is there a separate pre-registration step?

This is to prevent others from stealing your new name by registering it quickly themselves when they see your transaction. The name is not broadcasted during the pre-registration step, only a salted hash of it. There is a mandatory minimum delay of 12 blocks before you can broadcast your name with the registration step; this means that by the time other people know what name you're registering, they would have to reverse at least 12 blocks in order to steal the name.

## How are names represented?

Names and values are attached to special coins with a value of 0.01 NMC. Updates are performed by creating a transaction with the name's previous coin as input. Think of it like a colored coin. As far as Namecoin's consensus layer is concerned, names and their values are arbitrary binary blobs; any semantics assigned to those binary blobs (e.g. names being ASCII and values being JSON) are solely conventions used by higher-layer applications (e.g. ncdns).

## What if I spend that special coin by mistake?

The code prevents those coins from being used for normal payments.

## Why does registering a name incur a fee?

Fees on name operations are a rate-limiting mechanism to disincentivize squatting.

## Why don't name registration fees go to miners?

If name registration fees went to miners, it would enable an attack in which miners could register names at a discount compared to typical users. This would incentivize miners to sell discounted name registration services, which would enable miners to frontrun registrations that passed through such services, bypassing the frontrunning protections enabled by the [separate pre-registration step](#).

## Why do names have to be renewed regularly?

Two reasons:

1. It incentivizes owners of names who no longer intend to use them to either let them expire or sell them, thereby decreasing squatting.
2. It ensures that if a name owner loses their private keys, the name will eventually be returned to the pool of available names instead of permanently being stuck in limbo. Names being stuck in limbo would both pollute the namespace and be a security risk (since it would not be possible to revoke TLS keys for such names).

## Does Namecoin support “layer 2” technologies?

Yes. See our [Layer 2](#) documentation.

## Why focus on getting browsers and OS’s to support Namecoin instead of getting ISP’s or public DNS resolvers (e.g. Google DNS) to do so?

The reasons mostly fall under three categories: security concerns, usability concerns, and political concerns.

Security concerns:

- ISP’s would be in a position to censor names without easy detection.
- ISP’s would be in a position to serve fraudulent PKI data (e.g. TLSA records), which would enable ISP’s to easily wiretap users and infect users with malware.
- Either of the above security concerns would even endanger users who are running Namecoin locally, because it would make it much more difficult to detect misconfigured systems that are accidentally leaking Namecoin queries to the ISP. See this [case study](#) for a practical example of how this can happen.

Usability concerns:

- Namecoin-to-DNS bridges rely on DNS security protocols such as DNSSEC, DNS over TLS, or DNSCrypt to prevent tampering.
- Many local network firewalls break DNSSEC.
- Many ISP’s don’t support DNS over TLS or DNSCrypt.
- Many OS’s don’t support DNSSEC, DNS over TLS, or DNSCrypt.
- These compatibility issues are straightforward to solve by adding locally installed software (e.g. Dnssec-Trigger), but are not otherwise easily solvable

by non-technical users.

- If a non-technical user is installing DNS security software anyway, installing Namecoin as well doesn't add any particular extra difficulty.
- In the case of non-ISP public DNS resolvers, changing DNS settings manually in mainstream OS's is not something that non-technical users are usually comfortable doing, and is significantly more difficult to walk a user through than simply running a `.exe` file or installing a package via `apt-get`.

#### Political concerns:

- Namecoin's `.bit` TLD isn't part of the DNS; asking public DNS infrastructure to mirror Namecoin would probably be seen as hostile by IETF and ICANN.
- Namecoin is seeking to be added to IETF's special-use names registry; the precedent set by `.onion`'s inclusion is that public DNS infrastructure should always return `NXDOMAIN` for special-use names.
- While getting Namecoin bundled with a major browser or OS certainly is a major undertaking, it's not at all clear that getting Namecoin resolution included by a major ISP or public DNS resolver would be easier. Statistically (though exceptions certainly exist), software vendors tend to be more interested in innovating via software, security, and cryptography, whereas ISP's tend to be more interested in "innovating" via antitrust violations and net neutrality violations. We believe that software vendors are therefore more likely to be interested in Namecoin (though we don't claim that no ISP's exist who might be persuadable).

In addition, it's not clear that there would even be any significant benefit to counterbalance these concerns. Namecoin intentionally makes different tradeoffs from the DNS. For example, the DNS is much more scalable than Namecoin, can protect name owners from trivial deanonymization much better than Namecoin can, and doesn't rely on comparatively weak game-theoretic security properties as Namecoin does. Namecoin has some benefits that counterbalance these weaknesses (e.g. the non-reliance on trusted third parties), but serving Namecoin data from public DNS infrastructure would provide the **union** of Namecoin's and the DNS's weaknesses, while providing the **intersection** of Namecoin's and the DNS's strengths. Users who require a DNS-like naming system that works without any software installation are likely to be better off simply using the DNS.

## Why focus on browser add-ons and OS packages instead of native browser and OS support?

Because browser add-ons and OS packages are the standard method by which browser and OS vendors evaluate features for future inclusion. In our discussions with browser vendors and OS vendors (even the ones who are enthusiastic about bundling Namecoin by default), one of the first things they ask for as a prerequisite to inclusion by default is a browser add-on or an OS package.

## Why focus on getting existing browsers and OS's to support Namecoin instead of forking those browsers and OS's?

Maintaining a fork of a web browser or OS is a substantial time investment, and attempting it without the necessary resources would inevitably result in delayed security updates, which would be unethical to our users. Examples of browser and OS forks that have suffered from delayed security updates include IceCat and Trisquel. One of the very few cases where a web browser fork has not resulted in a security disaster is Tor Browser, which has the following advantages:

1. The Tor Project employs a dedicated team of full-time browser engineers who merge security fixes from Firefox.
2. Tor Browser is based on the ESR variant of Firefox, which results in significantly less code churn from upstream.
3. The Tor Browser developers are actively getting their patches against Firefox merged upstream by Mozilla.

These advantages do not obviously apply to us, so Tor Browser's relative success would not obviously apply to us either.

## Is Namecoin's support of atomic name trades a feature primarily aimed at squatters?

Short answer: No. The Namecoin developers are strongly against trademark infringement, and we do not endorse the behavior of users who squat on domains, either in Namecoin or the DNS.

Longer answer from a high-level point of view:

In a naming system, the ability to transfer ownership of a name to a new keypair has significant security benefits. For example, it allows a corporation to replace the employee(s) who control a name, and it also allows secure recovery of a name whose keys are believed to have been compromised but which has not yet been stolen. As a result, Namecoin supports the ability to transfer names to a new keypair. In a naming system that doesn't enforce legal identity verification, it is not possible to automatically disambiguate a transfer between two keypairs that belong to the same corporation or person from a transfer between two different people. As a result, Namecoin supports the ability to transfer names to a different corporation or person. Since it is always possible for two parties to coordinate a payment out-of-band, it is not possible for a cryptographic naming system to prevent name sales without preventing name donations. As a result, Namecoin supports the ability to sell a name. Given that Namecoin supports the ability to sell a name, there isn't really much benefit to not supporting atomic name sales: the only people who would benefit from not supporting atomic name sales are scammers. There are plenty of legitimate reasons why someone might want to sell a name (which we assume is the main reason why selling DNS names isn't banned, even though in the DNS it's usually quite easy on a technical level to seize domain names that are listed for sale). And we don't think that the legitimate users of that functionality deserve to be unnecessarily exposed to counterparty risk.

Longer answer from a low-level point of view:

Namecoin is a fork of Bitcoin, and therefore Namecoin (like Bitcoin) supports a wide variety of smart contract schemes, including the ability for a transaction to have an arbitrary number of outputs (thereby making multiple payments atomically). Because Namecoin represents names as transaction outputs, it is naturally possible to atomically transfer a name in combination with a currency payment. This isn't a feature that Namecoin was specifically designed to support, it's simply a feature that naturally exists, which would have required extra effort to not support. Technically, it would be possible to softfork Namecoin to ban name outputs from coexisting in a transaction with currency outputs, but in practice this would have detrimental effects unrelated to atomic name trades, because it would also ban change outputs from single-party name transactions. There *is* a restriction in Namecoin's consensus rules that prevents two name outputs from being created atomically. As far as we're aware, there is no documented reason for this rule (none

of us were around to ask when the rule was first created, and Vince isn't around for us to ask anymore), and this rule also has harmful side effects that are unrelated to atomic name trades, e.g. it prevents CoinJoin-style constructions for name transactions. Because CoinJoin is useful for both scalability and privacy, we would prefer that this rule be removed, and it is possible that a future consensus fork will do so.

## Does Namecoin have any browser add-ons?

Yes; we have a PKCS#11 module (ncp11) for TLS certificate validation, and we have a WebExtension (DNSSEC-HSTS) for protecting against SSLStrip attacks. However, there is no browser add-on for resolving [.bit](#) domains to IP addresses.

## Why doesn't Namecoin use a WebExtension to resolve [.bit](#) domains to IP addresses?

There is no WebExtensions API for intercepting DNS lookups; thus such a WebExtension is not possible. It *is* possible to abuse the HTTP proxy API to simulate DNS interception (and there are various 3rd-party WebExtensions that purport to do this for Namecoin). Unfortunately, this form of API abuse is fundamentally incompatible with HTTPS. Since such WebExtensions cannot work with HTTPS and are therefore inherently insecure, we recommend avoiding such WebExtensions. It also is possible to use the WebRequest API to redirect [.bit](#) URL's to the associated IP address. Unfortunately, this will not work with properly configured servers, because both the HTTP [Host](#) header and the TLS SNI header won't match; thus we recommend against this as well.

## Why doesn't Namecoin use "proof of stake"?

We defer to the analysis of Bitcoin developer Andrew Poelstra about the [security problems with PoS](#). For a more accessible summary, Namecoin developer [Yanmaani's article on PoS](#) may be of interest.

## Comparison of Namecoin to other projects

### What is the relationship of Namecoin to Bitcoin?

The Namecoin codebase consists of the Bitcoin codebase with relatively minor changes (~400 lines) and additional functionality built on top of it. The mining procedure is identical but the block chain is separate, thus creating Namecoin. This approach was taken because Bitcoin developers wanted to focus almost exclusively on making Bitcoin a viable *currency* while the Namecoin developers were interested in building a *naming system*. Because of the different intended use cases between the two projects, consensus and protocol rules might make sense in one but not the other. Examples of places where it could make sense to have different protocol or consensus rules:

- Namecoin's consensus rules need to enforce uniqueness of names. While it is possible to store data in Bitcoin (e.g. key/value pairs in **OP\_RETURN** outputs), uniqueness is not enforced by Bitcoin. It would be theoretically possible to build a layer on top of Bitcoin that discards **OP\_RETURN** outputs that don't respect uniqueness (e.g. a name operation that steals someone else's name), but any such layer would not be enforced by miners. If transaction validity rules are not enforced by miners, then they are not backed by **PoW**, which means that **SPV-based lightweight clients** will fail to enforce those validity rules.
- Since consumers expect different fees for financial transactions versus name registrations, and since the volume of financial transactions worldwide versus name registrations worldwide are different, Namecoin and Bitcoin might have different optimal block sizes.
- In a currency, inflation attacks are fatal, while in a naming system, they simply amount to a spamming or squatting attack: bad, but not anywhere near fatal. Therefore, decisions about features such as zk-SNARK-based anonymity (which introduce a risk of inflation attacks) might come to different conclusions between Namecoin and Bitcoin.
- Some script features that make sense for Namecoin might not make sense for Bitcoin, e.g. allowing a scriptPubKey to restrict the scriptPubKeys of any spending transaction. In a naming system, features like this could make renewing and updating names more convenient and secure, but in a currency, they could be harmful to fungibility.
- Coinbase commitments to the name database could be enforced by Namecoin consensus rules, allowing SPV proofs of a name's nonexistence to be created.

In general, the Namecoin developers attempt to minimize our patchset against Bitcoin. If a feature makes sense to have in Bitcoin, we try to get it into Bitcoin and then merge it to Namecoin; Namecoin usually only introduces differences from Bitcoin in cases where the proposed change wouldn't make sense for Bitcoin due to the differing use cases. Although it is theoretically possible to use Namecoin as a general-purpose currency, the Namecoin developers do not encourage this use case. There are lots of cryptocurrency projects out there that are specifically designed for such usage (e.g. Bitcoin); if you're looking for a currency, you should use one of those projects.

## What is the difference between Namecoin and Bitcoin?

- There are additional commands for special transactions containing *names* and *data* (key/value pairs).
- The most important commands are: `name_new`, `name_firstupdate`, and `name_update`.
- The coins used to pay for a `name_firstupdate` operation are destroyed, i.e. every new name reduces the finally usable maximum of 21 million NMC by 0.01 NMC.
- `name_new`, `name_firstupdate` and `name_update` contain a pair of name/value which expires after 36,000 blocks (between 200 and 250 days).
- The `d/` prefix is used to register a domain name, without the .bit TLD: { "name" : "d/opennic", "value" : "what you want", "expires\_in" : 10227 }
- The `id/` prefix is used to register an identity, see [NameID](#).
- Energy-efficient: if you are already mining bitcoins you can merge-mine namecoins at no extra cost for hardware and electricity. For a list of current Namecoin mining pools, see [our Metrics data](#).

## What are the similarities between Namecoin and Bitcoin?

- 21 million coins total, minus the lost coins.
- 50 coins are generated each block at the beginning; the reward halves each 210000 blocks (around 4 years).
- Security: a large fraction of Bitcoin miners also mine Namecoin, giving it a staggering difficulty.
- Pseudonymous founder: Vince, like Satoshi, never revealed his real-world identity and disappeared around the same time, leaving Namecoin project wild

in the open, to flourish only thanks to the help of enthusiasts in the FLOSS community.

- Free / libre / open-source platform: Anyone can improve the code and report issues on [GitHub](#) and even use it on other projects.

## Does Namecoin mandate usage of Bitcoin as a parent chain?

No. Namecoin's merged mining can use *any* Hashcash-SHA-256d blockchain as a parent chain. Bitcoin is the most commonly used such parent chain, but others (such as BCH) are sometimes used as parent chains as well. Note that this implies that Namecoin's hashrate and difficulty can theoretically be higher than those of Bitcoin. (In fact, Namecoin's 24-hour hashrate occasionally does exceed that of Bitcoin.)

## Does Namecoin influence Bitcoin's hashrate?

The existence of Namecoin as a merge-mined sidechain acts as a de facto increase of the Bitcoin block reward. This incentivizes mining Bitcoin at a higher difficulty than would otherwise be profitable. As a result, Namecoin indirectly increases Bitcoin's hashrate. Namecoin and Bitcoin hashrate are thus in a [mutualist](#) relationship. That said, since the real-world value of Namecoin's block reward is much less than that of Bitcoin's, the extent to which Namecoin increases Bitcoin's hashrate is relatively small. Specifically, as of 2022, Bitcoin's block reward was \$47,299,467.42 USD/day, while Namecoin's block reward was \$1,429.55 USD/day. Thus, Namecoin is responsible for a ~0.003% increase in Bitcoin hashrate. Namecoin's contribution might increase in the future as a result of increased adoption causing the exchange rate or transaction fees to increase. For example, in a hypothetical distant future in which all 368 million DNS second-level domains moved to Namecoin and paid \$10 USD/year in renewal fees, Namecoin's block reward would be \$10,075,291 USD/day, which would result in Namecoin contributing a 21.3% boost to Bitcoin hashrate.

## How does Namecoin compare to Tor Onion Services?

The Tor Project's Onion Services (which have a [.onion](#) top-level domain) use domains which are a public key hash. This means that their domain names are not human-meaningful, whereas Namecoin domain names are human-meaningful. Namecoin's [.bit](#) domains can point to [.onion](#) domains, providing a human-

meaningful naming layer on top of Tor Onion Services. Blockchain-based systems like Namecoin are, at this time, unable to match the cryptographic security guarantees (against impersonation or deanonymization attacks) that systems like Onion Service names provide when used directly, but Namecoin's human-meaningful names do make Namecoin more resistant than Onion Service names to some classes of attacks that exploit human psychology rather than breaking cryptography. For example, humans have trouble remembering a public key hash or recognizing a public key hash as the correct one; this is much better with meaningful names such as Namecoin names (or DNS names). Attackers can exploit this property of Onion Service names in order to trick users into visiting the incorrect website. We believe that both systems serve a useful purpose, and determining whether direct usage of Onion Service names or Namecoin naming for Onion Services is more secure for a given user requires consideration of that user's threat model.

## How does Namecoin compare to Let's Encrypt?

Let's Encrypt constitutes a trusted 3rd party, i.e. the Let's Encrypt certificate authority can issue fraudulent certificates to 3rd parties for your domain without your consent. In contrast, using TLS with Namecoin (assuming that negative certificate overrides are supported by your TLS client) does not involve a trusted 3rd party; only certificates that chain to a **TLSA** record in your name's value will be accepted.

Let's Encrypt also has the ability to censor your ability to receive TLS certificates. Let's Encrypt routinely uses this capacity to engage in geopolitical censorship. For example, in response to a [support request pertaining to an error "Policy forbids issuing for name"](#), Josh Aas (Executive Director of ISRG, the corporation that operates Let's Encrypt) stated on February 6, 2018:

The People's Republic of Donetsk is on the U.S. Treasury Department Specially Designated Nationals list. The website you are inquiring about appears to be a part of, or a state enterprise of, the People's Republic of Donetsk, thus we cannot provide service according to U.S. law.

Let's Encrypt also routinely censors journalism websites for political purposes. For example, on January 2, 2019, Let's Encrypt [revoked the TLS certificate for an allegedly-Russian-funded journalism website](#) aimed at American audiences, [on the grounds](#) that the website allegedly "engaged in efforts to post content focused on divisive political issues" and "attempted to hold a political rally in the United States".

[ISRG executive director Josh Aas](#) stated on January 4, 2019, that "This happens to maybe one domain per month".

In contrast, Namecoin does not have any 3rd party who can censor your ability to receive TLS certificates.

Let's Encrypt's services are entirely gratis. For Namecoin, the pricing is more complicated. In Namecoin, you create a private CA and place its public key into the blockchain; you can use that CA to issue as many certificates for your domain as you like without requiring additional blockchain transactions. Issuing certificates from your private CA (e.g. to rotate your TLS server's keys) is gratis. However, changing the set of private CA's (e.g. to immediately revoke old certificates before they expire) does require a blockchain transaction, which means you'll have to pay a transaction fee. The extra storage used by your private CA's public key also implies that renewing your domain name will incur a higher transaction fee than if you weren't using TLS.

TLS certificates issued by Let's Encrypt will work in most TLS clients (without security warnings) without any changes from defaults. In contrast, Namecoin TLS certificates will only work (without security warnings) if Namecoin is installed.

## How does Namecoin compare to Blockstack?

Below is a comparison table of Namecoin and Blockstack (with Bitcoin added for reference).

	Namecoin	Blockstack	Bitcoin
--	----------	------------	---------

	Namecoin	Blockstack	Bitcoin
Lightweight validation mode	SPV backed by PoW (e.g. BitcoinJ+libdohj or Electrum-NMC).	Checkpoints provided by a trusted 3rd party. Blockstack refers to this as “Consensus Hashes”, “SNV” (“Simplified Name Verification”), or (confusingly) “SPV”. Is not backed by PoW and has no relation to Bitcoin’s SPV threat model.	SPV backed by PoW (e.g. BitcoinJ or Electrum).
Hashrate attesting to transaction ordering	~95% of Bitcoin as of 2020 Jan 12.	100% of Bitcoin.	100% of Bitcoin.
Hashrate attesting to transaction validity	~95% of Bitcoin as of 2020 Jan 12.	0% of Bitcoin (miners do not attest to transaction validity).	100% of Bitcoin.
Miners possessing a majority of hashrate	None.	None.	None.
Mining pools influencing a majority of hashrate	None.	None.	None.
Legal jurisdictions influencing pools with a majority of hashrate	China.	China.	China.

	Namecoin	Blockstack	Bitcoin
Infrastructure capable of censoring all new blocks (non-selectively)	Bitcoin Relay Network, by censoring all Bitcoin blocks that commit to Namecoin blocks.	Bitcoin Relay Network.	Bitcoin Relay Network.
Infrastructure capable of censoring new blocks based on content (e.g. targeting a name)	None.	Bitcoin Relay Network.	Bitcoin Relay Network.
Scalability (blockchain download size, fully validating node)	6.06 GB as of 2020 Jan 12 ( <a href="#">source</a> ) (includes name values).	300.79 GB as of 2020 Jan 12 ( <a href="#">source</a> ), plus name values.	300.79 GB as of 2020 Jan 12 ( <a href="#">source</a> ).
Scalability (maximum name updates per hour)	~5494 to ~10989 (~546 on-chain bytes per update, block size limit 500 kB to 1 MB per ~10 minutes)	~4363 to ~6545 (~275 on-chain bytes per update, block size limit 200 kB to 300 kB per ~10 minutes)	N/A
Scalability (required incoming bandwidth for read operations, full block node)	500 kB to 1 MB per ~10 minutes (if blocks are full)	1 MB per ~10 minutes for Bitcoin parent chain (blocks usually full), plus all name operation data	1 MB per ~10 minutes (blocks usually full)

	<b>Namecoin</b>	<b>Blockstack</b>	<b>Bitcoin</b>
<b>Scalability (required incoming bandwidth for read operations, headers-only node)</b>	~1 kB to ~10 kB per ~10 minutes, plus a Merkle branch per read operation	Headers-only nodes not possible	80 B per ~10 minutes
<b>Consensus codebase</b>	Fork of Bitcoin Core with minimal changes (primarily merged mining and 3 new opcodes for altering a name database).	Codebase built by Blockstack developers.	Bitcoin Core.
<b>Blockchain type</b>	Is a sidechain (merge-mined with Bitcoin).	Developers have <a href="#">stated</a> that “the community needs to look into side chains” because Blockstack’s design won’t scale well.	Bitcoin.
<b>Parent blockchain agility</b>	Bitcoin is the de facto parent chain. If Bitcoin is attacked, dies out, or has other issues, miners can use a different Hashcash-SHA-256d parent chain without requiring any changes in Namecoin’s consensus rules (this worked in practice when BCH forked from Bitcoin). Non- Hashcash-SHA-256d parent chains could be adopted via a hardfork.	Bitcoin is the enforced parent chain. Using any non-Bitcoin parent chain requires a hardfork.	No parent chain.

	Namecoin	Blockstack	Bitcoin
<b>Data storage</b>	Choice between blockchain (similar threat model to Bitcoin; resistance to censorship is enforced as a consensus rule) and external storage (lower transaction fees, higher scalability). External DNS storage currently supports nameservers (threat model is DNSSEC with user-supplied keys; the DNSSEC keys have similar threat model to Bitcoin). External identity storage currently supports OpenPGP keyservers.	Required external storage; consensus rules do not enforce resistance to censorship.	Blockchain; resistance to censorship is enforced as a consensus rule.
<b>Namespace creation pricing</b>	Creating namespaces is open to all users, free of charge.	Creating a desirable namespace <b>costs a large amount of money</b> (0.4 BTC minimum; 40 BTC for a 2-character namespace).	N/A.
<b>Name pricing and name length</b>	All names have equal registration price.	Name registration price deterministically depends on length, character usage, and namespace.	N/A.
<b>Name pricing and exchange rates</b>	Price optimality is dependent on NMC/fiat exchange rates.	Price optimality is dependent on BTC/fiat exchange rates.	N/A.
<b>Names premixed?</b>	Not premixed.	Premixed.	N/A.
<b>Coins premixed?</b>	Not premixed.	Premixed via ICO (source). <b>Falsely claimed</b> that there would not be an ICO.	Not premixed.

	Namecoin	Blockstack	Bitcoin
<b>Funding sources and ethics</b>	Crowdfunding, donations, consulting/contracting (e.g. for F2Pool and an employee of Kraken). Has refused funding opportunities that were perceived to create conflicts of interest regarding user freedom, privacy, and security. Frequently references WikiLeaks and Ed Snowden in specification examples and other development discussion.	Business model is not publicly disclosed. <a href="#">Seed round</a> led by an investor who has <a href="#">endorsed cryptographic backdoors</a> and who considers <a href="#">ROT13</a> to be a “serious” and “intriguing” security mechanism, and another investor who has also <a href="#">endorsed cryptographic backdoors</a> .	(N/A)
<b>Do the developers run services that hold users’ private keys?</b>	No. Many years ago, a former Namecoin developer did run such a service. It has been discontinued, as the current Namecoin developer team considers such services to be harmful and a liability.	Yes, <a href="#">Onename</a> holds users’ private keys.	Not as far as we know.
<b>Patented by developers?</b>	Not patented by developers.	<a href="#">Patented by developers..</a> Developers did not disclose the patent to their users. As of 2017 Nov 20, Startpage for “patent”, “patented”, or Blockstack’s patent number shows zero hits on blockstack.org, nor does searching the Blockstack forum for those terms yield any hits.	Not patented by developers.

The Blockstack developers have demonstrated a repeated, consistent history of obfuscating their security model. Three examples:

Example 1: At launch, Blockstack used a DHT for data storage. See the opinions of Bitcoin developers [Peter Todd](#) and [Greg Maxwell](#) about DHT's. Namecoin developers publicly [warned](#) when Blockstack launched that DHT's were likely to be unsafe in Blockstack. Quoting the Namecoin blogpost from 2015 Sept. 29:

Additionally, DHT-based discovery of storage nodes is one of the classic suggestions of new users as an alternative to DNS seeds, and, originally, IRC-based discovery: it has never been committed because it is trivial to attack DHT-based networks, and partly because once a node is connected, Bitcoin (and thus Namecoin) peer nodes are solicitous with peer-sharing.

As an actual data store, DHT as it is classically described runs into issues with non-global or non-contiguous storage, with little to no way to verify the completeness of the data stored therein. With the decoupled headers in OP\_RETURN-using transactions in Bitcoin and the data storage in a DHT (or DHT-like) separate network, there is the likelihood of some little-used data simply disappearing entirely from the network. There is no indication of how Blockstore intends to handle this highly-likely failure condition.

In response to this criticism, Ryan Shea (Blockstack CEO) [stated](#) on 2015 Sept. 30:

Using a DHT could mean that data could become inaccessible

The information one gets from the DHT is hash-validated by the record in the blockchain which means you can get it from anywhere without trusting the source. The DHT is just one possible source of information and we have set up mirrors to ensure data redundancy and allow anyone to run a mirror in addition to a DHT node. Further, the data in the DHT gets periodically data mined and re-populated as needed by mirrors, to ensure there is no data loss whatsoever. This has been extensively tested.

Muneeb Ali (Blockstack CTO) also [stated](#) on 2015 Sept. 30 (emphasis in original):

Their DHT arguments show a lack of understanding of how Blockstore's storage works. They **incorrectly assume that the DHT doesn't have global state. It does.**

However, on 2017 Jan. 23, Muneeb Ali (Blockstack CTO) [posted](#) the following (link uses archive.is, which is not Tor-friendly, due to Blockstack apparently blocking the Tor-friendly archive.org Wayback Machine from archiving their forum):

Over this weekend (Jan 22), some community members (thanks, Albin!) reported “Data not saved in DHT” error for their profiles. I debugged this issue and turned out that some nodes of our DHT deployment were on a partition. This is very common in DHTs. We’ve been lucky in our deployment (which started in summer 2015 and has been running continuously since) and haven’t experienced partition issues that frequently. This is because of:

1. Active monitoring of default discovery nodes and throwing more RAM/CPU at the discovery nodes, so it’s hard to overwhelm them with requests.
2. Use of a caching layer where even if the underlying DHT network is experiencing, and recovering from, a partition read queries going to nodes that use a caching layer will still work for (heavily) cached data.
3. We can proactively check the blockchain for new data and check if data has propagated on the DHT network (traditional DHTs don’t have any such channel where new data writes get broadcasted).

Even with these additional monitoring and caching services, and extra information about new writes, we still experience issues. And the Atlas network described above helps a lot because it’s a fundamentally new design which, in my view, is much better than using a traditional DHT for our use case. Anyway, just restored the DHT partition and things are back to normal.

Blockstack subsequently stopped using a DHT; Muneeb Ali (Blockstack CTO) [stated](#) on 2017 Jan. 13 about why their proposed replacement (a custom P2P network called Atlas) is better than their DHT (emphasis in original; link uses archive.is, which is not Tor-friendly, due to Blockstack apparently blocking the Tor-friendly archive.org Wayback Machine from archiving their forum):

Atlas nodes have a **global view** of the state meaning that they know if they're missing any data items. This is because we use the blockchain to propagate information about new puts (new data items written to the network). This increases reliability a lot because traditional DHT nodes don't even know if they're missing data (there is no global view in traditional DHTs and there are theoretical proofs for that).

In other words, the exact issue whose existence we pointed out, and he denied, in 2015.

Example 2: Namecoin developers [pointed out](#) when Blockstack launched that Blockstack was incompatible with SPV. Ryan Shea (Blockstack CEO) [replied on Reddit](#) on 2015 Sept. 30:

Implementing SPV wouldn't be secure as it depends on having all block information

The short version is that blockstore definitely supports lightweight nodes. We'll be publishing a blog post on exactly how this works very soon.

Muneeb Ali (Blockstack CTO) also [claimed](#) on 2015 Sept. 30 (emphasis in original):

it is **possible to have SPV-like functionality** in Blockstore. We will publish details about it.

However, the Blockstack developers **already knew** that this was impossible; on 2014 Dec. 12 (before Namecoin developers pointed out the issue), Chris Pacia (an OpenBazaar developer collaborating with Blockstack) [stated](#) on the Blockstack issue tracker:

OK. I don't think a blockchain-only lightweight proof is possible without an additional consensus mechanism (blockchain). In fact, I think this is why counterparty and mastercoin don't have SPV implementations — because you can't do it.

The system that Blockstack ended up releasing was... trusted 3rd-party checkpoint hashes. Not remotely similar to SPV, and not something that most blockchain developers would refer to as a “lightweight node”.

Example 3: Namecoin developers have pointed out in this FAQ that Onename (Blockstack’s centralized web application for registering names) holds users’ private keys. On 2017 Apr. 07, Muneeb Ali (Blockstack CTO) [complained](#) about this, stating:

Private keys on Onename are encrypted with a password only the user has. So Onename doesn’t technically hold private keys, just encrypted blobs that are useless without the users’ passwords. In comparison, Coinbase actually holds private keys. Exchanges can send bitcoin without the user’s permission. This is not the case for Onename.

Namecoin developers initially pointed out that the web server could easily serve malicious JavaScript to steal private keys, and therefore Blockstack developers still had access to keys. However, it turned out to be even worse than that. Blockstack’s own documentation [states](#):

For new registration, the Onename webapp registers your username on Blockstack on your behalf and then transfers the ownership to you.

This implies that the Onename server controls the keys during the registration process, and could easily steal names while they’re being registered without serving malicious JavaScript. A quite different picture than what one might imagine from what Muneeb said to us.

Blockstack’s security model obfuscation raises serious questions about whether any future security claims by the Blockstack developers can be taken at face value.

## How does Namecoin compare to Monero?

Monero’s MoneroDNS project is similar in concept to Namecoin. MoneroDNS’s technical differences to Namecoin are similar to Monero’s technical differences to Bitcoin. Monero has had much less technical review than Bitcoin, and merge-mined chains based on Monero have significantly less hashrate security available to them than merge-mined chains based on Bitcoin. On the other hand, Monero’s small size

enables them to liberally experiment with more advanced features and cryptography, whereas Bitcoin-based systems like Namecoin are more conservative. The Namecoin and Monero development teams are cooperating on areas of common interest, as both projects agree that Namecoin and Monero both have a future.

## What is Namecoin's relationship to OpenNIC?

On May 27, 2014, OpenNIC [voted](#) to add a centralized Namecoin inproxy to their DNS infrastructure. No Namecoin developers participated in [the discussion](#) surrounding that vote.

On December 4, 2018, a brief [discussion](#) occurred within OpenNIC about whether Namecoin should be removed. The cited reason for considering removing Namecoin was that some OpenNIC server operators had been harassed by blacklist providers and hosting providers due to some botnet activity that was accessing OpenNIC for C&C infrastructure. The alleged botnet C&C domains included some Namecoin domains, but also included some centralized OpenNIC domains, such as domains on [.fur](#). OpenNIC criticized those blacklist providers for the harassment, saying “none of them have the courtesy to so much as send an email to abuse@domain to let you know that a problem was detected... they claim to be trying to protect the internet but don't give victims a chance to fix the problems”. The discussion “[produced] [little in the way of support or dissent](#)” for whether to continue resolving Namecoin domains, and OpenNIC decided to continue resolving Namecoin.

On December 19, 2018, [PRISM Break](#) lead maintainer Yana Timoshenko floated the idea to Namecoin developer Jeremy Rand of de-listing OpenNIC due to security concerns about centralized Namecoin resolution. Jeremy concurred that centralized Namecoin resolution was a security risk, pointed to a [case study](#) he had previously written on the subject, and recommended that PRISM Break not list centralized Namecoin resolvers; Yana removed OpenNIC from PRISM Break.

On June 9, 2019, Katie Holly from OpenNIC [contacted](#) Yana and Jeremy on the PRISM Break issue tracker, stated that she had recently discovered Yana's and Jeremy's concerns, and asked what OpenNIC would need to do to be re-listed on PRISM Break. Katie also said that OpenNIC would shortly hold an election on whether to remove Namecoin support as Yana and Jeremy had recommended.

On June 10, 2019, Yana replied, stating that removing centralized Namecoin resolution was of “critical” priority if OpenNIC was to be re-listed. Jeremy subsequently recommended the same.

On June 11, 2019, OpenNIC **announced** that they were beginning their election on whether to follow Yana’s and Jeremy’s recommendation to remove Namecoin support.

On June 25, 2019, Jeff Taylor from OpenNIC **announced** that the election had concluded in favor of following Yana’s and Jeremy’s recommendation, by a final margin of 13 to 2.

On July 30, 2019, Jeremy **published** a blogpost publicly thanking OpenNIC for doing the right thing. Yana signed off on the blogpost before publication. (The blogpost was written on June 30, but publication was delayed by the Tor Developer Meeting.)

There is currently no active relationship between Namecoin and OpenNIC, but some Namecoin developers (including Jeremy) continue to recommend OpenNIC to users who want a centralized naming system that isn’t run by ICANN.

## Weaknesses

### How easy is it for names to be stolen? What can be done if it happens?

For an attacker who does not have a majority of hashrate, stealing a Namecoin name is, roughly speaking, equivalent to the task of stealing bitcoins. This usually requires stealing the private key which owns the name. Assuming that proper security measures are in place by the owner, this is very difficult. However, if a user fails to keep their private keys safe, all bets are off. The standard method for attempting to steal bitcoins is to use malware; this is likely to be equally effective for stealing Namecoin names. Users can protect themselves using all the standard methods of avoiding malware, which are out of scope of this FAQ.

The good news is that the script system inherent in Bitcoin and Namecoin is designed to enable features that make theft more difficult. Many features are under development that would allow users considerable flexibility in constructing anti-theft policies that meet their needs. For example:

- **Multisig** (similar to Bitcoin) would allow names to be controlled by M-of-N keys. Some of these keys could belong to the various directors of a company, be stored in a secure location, or be stored by semi-trusted service providers. This is currently supported by the Namecoin protocol and consensus rules, but not well-exposed to end users.
- **Offline signing** (similar to Bitcoin) would allow names to be controlled by keys that are located on an air-gapped computer, an isolated offline Qubes virtual machine, or a hardware wallet. This is currently supported by the Namecoin protocol and consensus rules, but not well-exposed to end users.
- **Delegated renewal** (Namecoin-specific) would allow a key to be authorized to renew a name, but not change its value or its owner. Efforts are underway to add this to the Namecoin protocol and consensus rules.
- **Delegated alteration** (Namecoin-specific) would allow a key to be authorized to alter the value of a name, but not change its owner. This is supported, but not well exposed to end users. Further improvements are underway. See the docs on [delegated alteration](#).
- **Delegated partial alteration** (Namecoin-specific) would allow a key to be authorized to alter a specific subset of the value of a name (for example, be allowed to change a domain name's IP address but not its TLS certificate), but not change other parts of the value or its owner. This is supported, but not well-exposed to end users. Further improvements are underway. See the docs on [delegated alteration](#).

The above features can, of course, be combined arbitrarily for additional layered security.

Unfortunately, if all of the above security measures fail (or are not in use for a given name), and a name does get stolen, it is very difficult to recover it. Legal action might be able to fine or imprison the thief if they refuse to return the name, but this is not reliable, given that there is no guarantee that the thief will be identifiable, or that the thief will be in a legal jurisdiction who cares. Furthermore, since names do get sold or transferred on a regular basis, it would be difficult to prove that the name was not voluntarily transferred. (False claims of theft are problematic in Bitcoin too.) In cases where it is obvious that a theft has occurred (e.g. a previously reputable website starts serving malware), voluntary and user-

bypassable third-party blacklists (e.g. [PhishTank](#)) could be reasonably effective at protecting users in some circumstances. While this doesn't recover the name, it does reduce the incentive to attempt to steal names.

We are unaware of convincing empirical evidence of how Namecoin's theft risk compares to that of the DNS when the recommended security procedures of both are in use; this is difficult to measure because it is likely that a significant number of Namecoin users and DNS users are not using the recommended security procedures.

## What is the threat posed by 51% attacks?

Information about what a 51% attacker can do in Bitcoin is [described on the Bitcoin StackExchange](#). Namecoin is quite similar. The primary things that adversely affect Namecoin are reversing transactions sent by the attacker and preventing transactions from gaining confirmations.

Reversing transactions sent by the attacker would allow name registrations to be stolen if the reversed transaction is a `name_firstupdate`. This is because prior to being registered, names are considered to be "anyone can spend", meaning that prior to the registration, any arbitrary attacker is equally in ownership of a name as the user who actually registers it. Preventing transactions from gaining any confirmations would allow names to be stolen if all transactions for a name are prevented from confirming until the name expires after 36000 blocks, at which point the attacker can register it (but it should be noted that this would require a prolonged 51% attack lasting until the 36000-block expiry period elapses, which would be highly expensive).

Both of these attacks are detectable. In the case of reversing transactions, the evidence would be an extremely long fork in the blockchain, possibly thousands of blocks long or longer. In the case of preventing transactions from confirming, the evidence would be that the blockchain indicates that a name expired and was re-registered. In both cases, it is detectable which names were attacked. In the case of preventing transactions from confirming, it is also possible for the legitimate owner of the stolen name to register a new name after the attack is over, and sign it with the owner key of the original name, thus proving common ownership and allowing secure resurrection of the name. The only way to prevent this resurrection is for the attacker to continue to expend mining resources on the attack for as long as they

with to prevent the name from being resurrected. In the case of reversing transactions, it is not possible to prove ownership of the original name and resurrect it. Luckily, reversing old transactions is considerably more expensive than preventing new transactions from confirming.

It is noteworthy that a 51% attacker cannot sell a name to a user and then steal back the name. Nor can a 51% attacker buy a name from a seller and then steal back the money. This is because Namecoin supports *atomic* name trades: reversing the purchase payment also reverses the name transfer, and vice versa. Double-spending of `name_update` transactions also isn't beneficial to an attacker, because `name_update` transactions typically are sent by a user to themselves, meaning that the attacker could only scam themselves.

In both Bitcoin and Namecoin, the Chinese government has jurisdiction over a majority of hashpower. This is problematic for both Bitcoin and Namecoin, and should be fixed in both. Because not all Bitcoin miners also mine Namecoin, F2Pool previously had a majority of Namecoin hashpower (they no longer do). This was also problematic when it was the case. However, in practice, the Chinese government has considerably more motivation to perform a 51% attack than F2Pool does. (The Chinese government has a [history of messing with Internet traffic](#). F2Pool has supported Namecoin development both financially and logistically, which makes it unlikely that they would want to attack it.)

A majority of Bitcoin's hashpower is routed via the Bitcoin Relay Network, which has the ability to censor Bitcoin blocks that pass through it. This produces incentives for Bitcoin miners to self-censor any blocks that might violate any policy introduced in the future by Bitcoin Relay Network, because routing blocks through Bitcoin Relay Network reduces orphan rates for miners. Namecoin's blocks are much smaller than Bitcoin's, and therefore Namecoin does not have similar incentives for centralized block relay infrastructure. While it is possible for Bitcoin Relay Network to attack Namecoin by censoring Bitcoin blocks that commit to merge-mined Namecoin blocks, it is not feasible for Bitcoin Relay Network to look inside the Namecoin blocks that are committed to, which means that Bitcoin Relay Network cannot censor Namecoin blocks by content as they can with Bitcoin blocks. Bitcoin Relay Network is operated by Bitcoin Core developer Matt Corallo, who is unlikely to want to attack Bitcoin (just as F2Pool is unlikely to want to attack Namecoin).

The takeaway here is that while F2Pool theoretically used to be capable of attacking Namecoin (but not Bitcoin), and Bitcoin Relay Network is theoretically capable of attacking Bitcoin (but not Namecoin), *in practice* the party with the most motivation to attack either chain (the Chinese government) has jurisdiction over a hashrate majority of both Bitcoin and Namecoin. Mining decentralization is an active research area, and we hope that significant improvements in this area are made, as they would improve the security of both Bitcoin and Namecoin.

## Is squatting a problem? What can be done about it?

There are several types of squatting concerns sometimes raised in relation to Namecoin.

The first concern is that too many potentially high-value domains, e.g. [d/google](#), have been squatted for the purpose of resale. This is not a problem that can be solved in a decentralized system, because “squatting on [d/google](#)” is defined as “owning [d/google](#) while not being the real-world company named Google”, and determining that a given name is or is not owned by a given real-world entity requires some trusted party. Raising the price of names wouldn’t have any effect on this, because no matter what the cost of registering a name is, the resale value of [d/google](#) is likely to be higher.

The second concern is that too many potentially high-value domains have been squatted for the purpose of impersonation. This is not a problem specific to Namecoin; phishing sites exist in the DNS world too, and are frequently countered by using systems such as web-of-trust and voluntary user-bypassable third-party blacklists (e.g. [PhishTank](#)). There is no reason to think that similar counters would not work in Namecoin.

The third concern is that single entities can squat on a large number of names, which introduces centralization into the space of squatted names. For comparison, DNS domain names are squatted a lot, but the space of squatted names is very decentralized, which reduces abusive behavior such as would happen if most squatted names belonged to one of a few people. This concern could be resolved by raising the price of name registrations, so that a squatter with a given investment budget cannot register as many names without selling or otherwise using them to recoup costs. While raising prices sounds like a great plan, the devil is in the details: increasing prices constitutes a softfork, and decreasing prices

constitutes a hardfork. Since cryptocurrencies like Namecoin have an exchange rate that varies over time, the optimal name price might need regular adjustment. There is ongoing research into how regular name price adjustment could be done safely and non-disruptively, and research in the wider cryptocurrency world on block size adjustment (which is a similar problem in many ways) may be applicable.

At the moment, the current developers consider other issues to be somewhat higher priority. For example, getting a domain name without dealing with squatters doesn't mean much if it's difficult for people to view your website. Once development of other areas has progressed further, we do intend to spend a larger fraction of our time on improving name pricing. However, if new developers want to get involved with proposing, prototyping, or analyzing name price systems, we would be delighted to have the assistance.

In the meantime, practical advice is that if you want a name but it's squatted, try to contact the owner (many squatters leave contact information in the value of their names) and see if they'll let you have it. We have heard of many cases where squatters either gave away names or sold them for very little money if the recipient actually planned to use the name rather than resell it. If they demand money that you're unwilling to pay, consider registering a different name. It's unlikely that the website or service you want to set up can only work with that one specific name. Strategies for finding an unused DNS domain name or an untrademarked business name are likely to be applicable for Namecoin too.

## Is Namecoin anonymous?

Like Bitcoin, Namecoin is not anonymous. A thorough description of Bitcoin's poor anonymity properties is outside the scope of this FAQ.

When used properly in conjunction with Tor, Namecoin *may* offer sufficient pseudonymity or location-anonymity for many use cases. Users who need these properties are advised to carefully evaluate their specific situation. Using Namecoin over Tor does *not* by itself magically make you anonymous.

We recognize that better anonymity is an important use case. We occasionally receive questions from users about whether Namecoin can be used anonymously. While we don't know much about these users (for obvious reasons), some of them

appear to be in circumstances where failure of anonymity could lead to significant negative consequences. We aim to support these use cases in the future, but right now it would be irresponsible and reckless to do so.

We are currently engaging with projects that provide blockchain anonymity (e.g. Monero and Zcash), with the goal of achieving similar anonymity for Namecoin. Both Monero and Zcash have mathematical security proofs of their anonymity, subject to given assumptions and a given anonymity set. Blockchain anonymity is also an active research area, so further innovations may very well occur in the future.

I heard that an academic study found that Namecoin is only used by 28 websites; is that really true?

This claim is derived from a study out of Princeton University, and is a result of faulty study design. The study's design considers all **.bit** websites that contain identical content to a DNS website to be "trivial" and discounts such websites, leaving only 28 **.bit** websites that contain content that cannot be found on a DNS website. This number seems plausible to us, though we haven't tried to reproduce the result independently. However, the Namecoin developers have never recommended that typical **.bit** domain owners restrict their website to only **.bit**; we usually recommend that **.bit** be used **in addition to** DNS. Reading Sec. 4.3 of the study reveals that the study authors found an additional 111 **.bit** domains that pointed to a website that was also available via DNS. This results in a total count of 139 **.bit** domains with non-trivial content, if the definition of "trivial" doesn't include websites that are available on both Namecoin and DNS. This count of 139 also seems plausible to us, though (again) we haven't tried to reproduce the result independently.

It is unfortunate that the Princeton study authors primarily marketed the count of 28 despite the count of 139 being a far more relevant measure. It is also unfortunate that the study authors did not contact us to ask for peer review, as we would have easily caught that issue had we been consulted. (Interestingly, the study authors *did* contact the CTO of a Namecoin competitor to ask for feedback on their paper prior to publishing.)

How does Namecoin affect global heating?

Namecoin does mildly increase Bitcoin's hashrate, which incentivizes greater electricity consumption by Bitcoin mining. However, this increase in electricity consumption is quite small compared to what Bitcoin would consume without Namecoin, because Namecoin's block reward is of much lower real-world value than Bitcoin's. Thus, Namecoin is not a major contributor to Bitcoin's electricity usage. Specifically, of the 39 Mt CO<sub>2</sub>e net emissions produced by Bitcoin+Namecoin mining in 2021, Namecoin was responsible for ~1.2 kt (0.003%). Of the S&P 500 companies, only 4 have a lower greenhouse footprint (each) than Namecoin mining. In addition, most Bitcoin mining is powered by renewable electricity sources, so Namecoin and Bitcoin are not a major cause of global heating. For information about Bitcoin mining's electricity usage, these articles may be informative:

- The reports of bitcoin environmental damage are garbage (Robert Sharratt, Jan. 2019)
- RE: Cost of Bitcoin Mining Misconceptions (Christopher Bendiksen, Jun. 2018)
- An Honest Explanation of Price, Hashrate & Bitcoin Mining Network Dynamics (Christopher Bendiksen, Nov. 2018)
- Beware of Lazy Research: Let's Talk Electricity Waste & How Bitcoin Mining Can Power A Renewable Energy Renaissance (Christopher Bendiksen, Dec. 2018)
- Surprise: Majority of BTC Energy Sourced from Hydro / Wind / Solar (Christopher Bendiksen, Jun. 2019)
- Bitcoin's Hash Rate Grew More Than 80% Since June — Mostly Within China (Christopher Bendiksen, Dec. 2019)
- Everything You've Heard About Bitcoin Mining and the Environment is Wrong (Christopher Bendiksen, Feb. 2022)
- The Bitcoin Mining Network: Trends, Marginal Creation Costs, Electricity Consumption & Sources (May 2018 Update) (CoinShares Research)
- The Bitcoin Mining Network: Trends, Marginal Creation Costs, Electricity Consumption & Sources (Nov. 2018 Update) (CoinShares Research)
- The Bitcoin Mining Network: Trends, Average Creation Costs, Electricity Consumption & Sources (Jun. 2019 Update) (CoinShares Research)
- The Bitcoin Mining Network: Trends, Average Creation Costs, Electricity Consumption & Sources (Dec. 2019 Update) (CoinShares Research)
- The Bitcoin Mining Network: Energy and Carbon Impact (Jan. 2022) (CoinShares Research)

Both Bitcoin and Namecoin also have second-order effects that oppose global heating. For example, Bitcoin decreases the influence of the Petrodollar (the Petrodollar is a major reason why the U.S. establishment opposes renewable energy sources), and Namecoin helps fight surveillance (climate activists are heavily targeted by government surveillance).